Constructor-based Inductive Theorem Prover (CITP) - part 1

Lecture Note 03

December 27, 2013

Introduction

- tool for proving inductive properties of **Observational Transition Systems (OTS)**
- implemented on top of **Maude**
  `http://www.jaist.ac.jp/~danielmg/citp.html`
- underlying logic - **constructor-based order-sorted preorder algebra**

Specifications

$$\mathrm{SP}\begin{cases}\text{signature } \mathbb{S}\mathit{ig}(\mathrm{SP}) \\ \text{set of axioms } \mathbb{A}\mathit{x}(\mathrm{SP}) \\ \text{class of models } \mathbb{M}\mathit{od}(\mathrm{SP})\end{cases}$$

A specification is constructed from

1. basic specifications (Σ, Γ) by applying
2. specification building operators

Order-Sorted Signatures

Order-sorted signature $(S, \leq, F, F^c)$:

$$\begin{cases} 1. & S & \text{– set of sorts} \\ 2. & (S, \leq) & \text{– poset} \\ 3. & F = (F_{w \to s})_{w \in S^*, s \in S} & \text{– funct. symb.} \\ 4. & F^c \subseteq F & \text{– constructors} \end{cases}$$

Assumptions:

each $(S, \leq, F, F^c)$ is sensible: for all $\begin{pmatrix} \bullet & \sigma \in F_{w \to s} \\ \bullet & \sigma \in F_{w' \to s'} \\ \bullet & w \equiv_{\leq} w' \end{pmatrix}$ we have $s \equiv_{\leq} s'$

Numbers

Example

```
mod* NUMBERS
{ [Zero < Nat]
op 0 :  -> Zero {constr}
op s_ :  Nat -> Nat {constr}
op _+_ :  Nat Nat -> Nat
}
```

$\mathbb{S}ig$(NUMBERS):

- **constrained** sorts:
  - `Zero` has one constructor `{0 :  -> Zero}`
  - `Nat` has two constructors `{0 :  -> Zero, s_ :  Nat -> Nat}`
- no **loose** sorts
- **constructor terms** (formed from constructors and variables of loose sorts):
  `0, s 0, s s 0,...`

Lists

Example

```
mod!  LIST
{ [Elt Empty < List]
op empty :  -> Empty {constr}
op con :  Elt List -> List {constr}
}
```

$\mathbb{S}ig$(LIST):

- **constrained** sorts:
  - Empty has one constructor {empty : -> Empty}
  - List has two constructors
  {empty : -> Empty, con : Elt List -> List}
- **loose** sorts : Elt
- **constructor terms** (formed from constructors and variables of loose sorts):
  empty, con(X1,empty), con(X2,con(X1,empty)),
  con(X3,con(X2,con(X1,empty))), ...

Order-Sorted Algebras

$$(S, \leq, F)\textbf{-algebras } A: \begin{cases} 1. & s \in S & \rightsquigarrow & A_s \\ 2. & s \leq s' & \rightsquigarrow & A_s \subseteq A_{s'} \\ 3. & \sigma : w \to s & \rightsquigarrow & A_{\sigma : w \to s} : A_w \to A_s \end{cases} \quad \text{such that}$$

functions "agree" on common arguments:

$$\text{for all} \left(\begin{array}{ll} \bullet & \sigma : w \to s \\ \bullet & \sigma : w' \to s' \\ \bullet & w \equiv_{\leq} w' \\ \bullet & \bar{a} \in A_w \cap A_{w'} \end{array} \right) \text{ we have } A_{\sigma : w \to s}(\bar{a}) = A_{\sigma : w' \to s'}(\bar{a})$$

Example

```
mod* NUM
{ [Zero < Nat]
op 0 :  -> Zero
op s_ :  Nat -> Nat
op _+_ :  Nat Nat -> Nat
}
```

$\mathbb{S}ig(\texttt{NUM})$-algebras:

- Natural numbers $\mathbb{N}$
$$\begin{cases} \bullet & \mathbb{N}_{\texttt{Zero}} = \{0\} \\ \bullet & \mathbb{N}_{\texttt{Nat}} = \{0, 1, 2, \ldots\} \\ \bullet & \mathbb{N}_{0} = 0 \\ \bullet & \mathbb{N}_{s} : \mathbb{N}_{\texttt{Nat}} \to \mathbb{N}_{\texttt{Nat}}, \qquad \mathbb{N}_{s}(n) = n + 1 \\ \bullet & \mathbb{N}_{+} : \mathbb{N}_{\texttt{Nat}} \times \mathbb{N}_{\texttt{Nat}} \to \mathbb{N}_{\texttt{Nat}}, \quad \mathbb{N}_{+}(n, m) = n + m \end{cases}$$

Order-Sorted Algebras

- Integers $\mathbb{Z}$
$$\begin{cases} \bullet\ \mathbb{Z}_{\texttt{Zero}} = \{0\} \\ \bullet\ \mathbb{Z}_{\texttt{Nat}} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \\ \bullet\ \mathbb{Z}_{0} = 0 \\ \bullet\ \mathbb{Z}_{\texttt{s}} : \mathbb{Z}_{\texttt{Nat}} \to \mathbb{Z}_{\texttt{Nat}}, \quad \mathbb{Z}_{\texttt{s}}(n) = n + 1 \\ \bullet\ \mathbb{Z}_{+} : \mathbb{Z}_{\texttt{Nat}} \times \mathbb{Z}_{\texttt{Nat}} \to \mathbb{Z}_{\texttt{Nat}}, \quad \mathbb{Z}_{+}(n, m) = n + m \end{cases}$$

- $\mathbb{Z}_2$
$$\begin{cases} \bullet\ (\mathbb{Z}_2)_{\texttt{Zero}} = \{\hat{0}\}, \\ \bullet\ (\mathbb{Z}_2)_{\texttt{Nat}} = \{\hat{0}, \hat{1}\} \\ \bullet\ (\mathbb{Z}_2)_{0} = \hat{0} \\ \bullet\ (\mathbb{Z}_2)_{\texttt{s}} : (\mathbb{Z}_2)_{\texttt{Nat}} \to (\mathbb{Z}_2)_{\texttt{Nat}}, \quad \begin{array}{l} (\mathbb{Z}_2)_{\texttt{s}}(\hat{0}) = \hat{1} \\ (\mathbb{Z}_2)_{\texttt{s}}(\hat{1}) = \hat{0} \end{array} \\ \bullet\ (\mathbb{Z}_2)_{+} : (\mathbb{Z}_2)_{\texttt{Nat}} \times (\mathbb{Z}_2)_{\texttt{Nat}} \to (\mathbb{Z}_2)_{\texttt{Nat}}, \quad \begin{array}{l} (\mathbb{Z}_2)_{+}(\hat{0}, \hat{0}) = (\mathbb{Z}_2)_{+}(\hat{1}, \hat{1}) = \hat{0} \\ (\mathbb{Z}_2)_{+}(\hat{0}, \hat{1}) = (\mathbb{Z}_2)_{+}(\hat{1}, \hat{0}) = \hat{1} \end{array} \end{cases}$$

- **ground terms** have unique interpretations into the models

$$\mathrm{ss0} + (\mathrm{0} + \mathrm{s0}) \rightsquigarrow \begin{cases} \overset{\mathbb{N}}{\rightsquigarrow} & 3 \\ \overset{\mathbb{Z}}{\rightsquigarrow} & 3 \\ \overset{\mathbb{Z}_2}{\rightsquigarrow} & \hat{1} \end{cases}$$

- **terms with variables** have one interpretation for each valuation of the variables

$$\mathrm{s}(\mathrm{sx} + \mathrm{y}) \rightsquigarrow \begin{cases} \overset{\mathbb{N}}{\rightsquigarrow}_f & 11 & \text{where } f : \{x, y\} \to \mathbb{N}, & \begin{array}{l} f(x) = 2 \\ f(y) = 7 \end{array} \\ \overset{\mathbb{Z}}{\rightsquigarrow}_g & 8 & \text{where } g : \{x, y\} \to \mathbb{Z}, & \begin{array}{l} g(x) = 5 \\ g(y) = 1 \end{array} \\ \overset{\mathbb{Z}_2}{\rightsquigarrow}_h & \hat{1} & \text{where } h : \{x, y\} \to \mathbb{Z}_2, & \begin{array}{l} h(x) = \hat{0} \\ h(y) = \hat{1} \end{array} \end{cases}$$

Term Algebra

$\Sigma = (S, \leq, F)$ sensible. T_Σ is defined recursively:

1.
   - $F_{\to s} \subseteq (T_\Sigma)_s$
   - $$\left.\begin{array}{l} \sigma \in F_{s_1 \ldots s_n \to s} \\ t_1 \in (T_\Sigma)_{s_1} \\ \vdots \\ t_n \in (T_\Sigma)_{s_n} \end{array}\right\} \Rightarrow \sigma(t_1, \ldots, t_n) \in (T_\Sigma)_s$$
   - $s \leq s' \Rightarrow (T_\Sigma)_s \subseteq (T_\Sigma)_{s'}$
2. if $\sigma \in F_{s_1 \ldots s_n \to s}$ the $(T_\Sigma)_\sigma : (T_\Sigma)_{s_1} \times \ldots \times (T_\Sigma)_{s_n} \to (T_\Sigma)_s$ is defined by $(T_\Sigma)_\sigma(t_1, \ldots, t_n) = \sigma(t_1, \ldots, t_n)$

Satisfaction Relation

A is a $(S, \leq, F)$-algebra

- $A \models_{(S,\leq,F)} (\forall X)(l = r)$ `if` $(u_1 = v_1) \bigwedge \ldots \bigwedge (u_n = v_n)$ iff

$$\text{for all } f : X \to A \text{ we have } \left.\begin{array}{l} A^f_{u_1} = A^f_{v_1} \\ \vdots \\ A^f_{u_n} = A^f_{v'_n} \end{array}\right\} \Rightarrow A^f_l = A^f_r$$

- $E \models_{(S,\leq,F)} \varepsilon$ iff for all $(S, \leq, F)$-models A we have $A \models_{(S,\leq,F)} E$ implies $A \models_{(S,\leq,F)} \varepsilon$

Reachable Order-Sorted Algebras

- **Reachable** $(S, \leq, F, F^c)$**-algebras** consist of interpretations of constructor terms

  A is reachable iff for all $a \in A$ there is $\left(\begin{array}{ll} \bullet & \text{constructor term } t[x_1, \ldots, x_n] \\ \bullet & \text{valuation } f : \{x_1, \ldots, x_n\} \to A \end{array} \right)$ s.t.

  $$A^f_{t[x_1,\ldots,x_n]} \overset{def}{=} A_{t[x_1 \leftarrow f(x_1),\ldots,x_n \leftarrow f(x_n)]} = a$$

- $E \models_{(S,\leq,F,F^c)} \varepsilon$ iff for all $(S, \leq, F, F^c)$-models A we have $A \models_{(S,\leq,F,F^c)} E$ implies $A \models_{(S,\leq,F,F^c)} \varepsilon$

Remark

- $\mathbb{N}$ is a reachable $\mathbb{S}ig(\mathrm{NUMBERS})$-algebra: for all $n \in \mathbb{N}$ we have $\mathbb{N}_{(\mathtt{s}^n \mathtt{0})} = n$
- $\mathbb{Z}$ is not reachable: there is no constructor term $\mathtt{s}^n \mathtt{0}$ such that $\mathbb{Z}_{(\mathtt{s}^n \mathtt{0})} = -1$
- $\mathbb{Z}_2$ is reachable: $(\mathbb{Z}_2)_{\mathtt{0}} = \hat{0}$ and $(\mathbb{Z}_2)_{\mathtt{1}} = \hat{1}$
- $T_{\mathbb{S}ig(\mathrm{NUMBERS})}$ is not reachable: there is no constr. term $\mathtt{s}^n \mathtt{0}$ s.t. $(T_{\mathbb{S}ig(\mathrm{NUMBERS})})_{\mathtt{s}^n \mathtt{0}} = \mathtt{0} + \mathtt{0}$

Basic Specifications

$\text{SP} = ((S, \leq, F, F^c), E)$

- $\mathbb{S}ig(\text{SP}) = (S, \leq, F, F^c)$
- $\mathbb{A}x(\text{SP}) = E$
- $\mathbb{M}od(\text{SP}) = \{A \in \mathbb{M}od(S, \leq, F, F^c) \mid A \models E\}$
  consists of all reachable algebras satisfying E

Example

```
mod* NUMBERS+
{ [Zero < Nat]
op 0 :  -> Zero {constr}
op s_ :  Nat -> Nat {constr}
op _+_ :  Nat Nat -> Nat
vars M N : Nat .
eq 0 + N = N .
eq s M + N = s(M + N) . }
```

SUM

- SP_1, SP_2 specifications s.t. $\mathit{Sig}(\mathrm{SP}_1) = \mathbb{S}\mathit{ig}(\mathrm{SP}_2) = \Sigma$
- $\mathrm{SP}_1 \cup \mathrm{SP}_2$ the summation of SP_1 and SP_2
  1. $\mathbb{S}\mathit{ig}(\mathrm{SP}_1 \cup \mathrm{SP}_2) = \Sigma$
  2. $\mathbb{A}x(\mathrm{SP}_1 \cup \mathrm{SP}_2) = \mathbb{A}x(\mathrm{SP}_1) \cup \mathbb{A}x(\mathrm{SP}_2)$
  3. $\mathbb{M}\mathit{od}(\mathrm{SP}_1 \cup \mathrm{SP}_2) = \mathbb{M}\mathit{od}(\mathrm{SP}_1) \cap \mathbb{M}\mathit{od}(\mathrm{SP}_2)$

TRANS

- $\mathbb{S}ig(\mathrm{SP}) \overset{\iota}{\hookrightarrow} \Sigma$
- $\mathrm{SP} * \iota$ the translation of SP by ι
  1. $\mathbb{S}ig(\mathrm{SP} * \iota) = \Sigma$
  2. $\mathbb{A}x(\mathrm{SP}) = \iota(\mathbb{A}x(\mathrm{SP})) = \mathbb{A}x(\mathrm{SP})$
  3. $\mathbb{M}od(\mathrm{SP} * \iota) = \{M \in \mathbb{M}od(\Sigma) \mid M{\restriction}_{\mathbb{S}ig(\mathrm{SP})} \in \mathbb{M}od(\mathrm{SP})\}$

$\mathrm{SP} * \iota$-models consists of
- SP-models
  $+$
- interpretation of the new symbols in Σ

Remark

If SP is formed from basic specification, SUM, and TRANS then SP is equivalent to $(\mathbb{S}ig(\mathrm{SP}), E)$, where E is a set of conditional equations.

Example

```
mod* NUMBERS+*                          mod* PNAT+*
{ protecting NUMBERS+                   { protecting PNAT+
op _*_ :  Nat Nat -> Nat .              op _*_ :  Nat Nat -> Nat .
eq 0 * N = 0 .                          eq 0 * N = 0 .
eq s M * N = (M * N) + N . }            eq s M * N = (M * N) + N . }
```

- $\mathbb{N}, \mathbb{Z}_2, \mathbb{Z}_3, \ldots \in \mathbb{M}od(\text{NUMBERS} + *)$, where the algebras $\mathbb{N}, \mathbb{Z}_n$ interprets `_*_ : Nat Nat -> Nat` in the obvious way
- $\mathbb{N} \in \mathbb{M}od(\text{PNAT} + *)$, $\mathbb{Z}_n \notin \mathbb{M}od(\text{PNAT} + *)$

Initiality

$\Sigma = (S, \leq, F, F^c)$ sensible.

1. **Σ-congruence** $\equiv = (\equiv_s)_{s \in S}$ on a Σ-algebra A
   - $\equiv_s$ is an equivalence relation on A_s (reflexive, symmetric and transitive)
   - $$\left.\begin{array}{l} \sigma \in F_{s_1 \ldots s_n \to s} \\ a_1 \equiv_{s_1} a'_1 \\ \vdots \\ a_n \equiv_{s_n} a'_n \end{array}\right\} \Rightarrow \boxed{A_\sigma(a_1, \ldots, a_n) \equiv_s A_\sigma(a'_1, \ldots, a'_n)}$$
   - if $s \leq s'$ then $\boxed{a \equiv_s a' \text{ iff } a \equiv_{s'} a'}$
2. **Quotient algebra** $A_\equiv$
   - $(A_\equiv)_s = (A_s)_{\equiv_s}$
   - $(A_\equiv)_\sigma : (A_\equiv)_{s_1} \times (A_\equiv)_{s_n} \to (A_\equiv)_s$ is defined by
     $(A_\equiv)_\sigma(a_1/\equiv_{s_1}, \ldots, a_n/\equiv_{s_n}) = A_\sigma(a_1, \ldots, a_n)/\equiv_s$

- E set of conditional Σ-equations: $\boxed{t \equiv_E t' \text{ iff } E \models t = t'}$
- $(T_\Sigma)_{\equiv_E}$ is reachable if (Σ, E) is sufficient complete

Definition (Sufficient Completeness)

$\mathtt{SP}$ is sufficient complete if for all $t \in T_{\mathbb{S}ig(\mathtt{SP})}$ there exists a constructor term $t' \in T_{\mathbb{S}ig(\mathtt{SP})}$ s.t. $\mathtt{SP} \models t = t'$.

- NUMBERS is not sufficient complete (_ + _ is underspecified)
- NUMBERS+ is suff. complete which implies that it has initial model.

```
mod* NUMBERS+
{ [Zero < Nat]
op 0 : -> Zero {constr}
op s_ : Nat -> Nat {constr}
op _ + _ : Nat Nat -> Nat
vars M N : Nat .
eq 0 + N = N .
eq s M + N = s(M + N) . }
```

```
mod! PNAT+
{ [Zero < Nat]
op 0 : -> Zero {constr}
op s_ : Nat -> Nat {constr}
op _ + _ : Nat Nat -> Nat
vars M N : Nat .
eq 0 + N = N .
eq s M + N = s(M + N) . }
```

Exercise

Prove that NUMBERS+ is sufficient complete.